Decoy-state quantum key distribution with both source errors and statistical fluctuations

Xiang-Bin Wang,[1,2] Lin Yang,[1,3] Cheng-Zhi Peng,[1,4] and Jian-Wei Pan[1,4,5]

[1]*Department of Physics, Tsinghua University, Beijing 100084, China*

[2] *Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, China*

[3]*Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China*

[4]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[5]*Physikalisches Institut, Universität Heidelberg, Philosophenweg 12, 69120 Heidelberg, Germany*

Abstract

We show how to calculate the fraction of single photon counts of the 3-intensity decoy-state quantum cryptography faithfully with both statistical fluctuations and source errors. Our results only rely on the bound values of a few parameters of the states of pulses.

PACS numbers: 03.67.Dd, 42.81.Gs, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD)[1, 2, 3, 4, 5, 6, 7] has now been extensively studied both theoretically and experimentally. In practice, if one uses an imperfect single-photon source with a lossy channel, the security is undermined by the photon-number-splitting attack [8, 9]. Fortunately, this can be managed by a number of methods[4, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]. In particular, the so called ILM-GLLP proof[4, 5] has shown that if we know the upper bound of fraction of the multi-photon counts (or equivalently, the lower bound of single-photon counts) among all raw bits, we still have a way to distill the secure final key. Verifying such a bound is strongly non-trivial. The so called decoy-state method [10, 11, 12, 13, 14] is to find out such bounds, say, among all those clicks at Bob's side, at least how many of them are due to the single-photon pulses from Alice.

The main idea of the decoy-state method is to change intensities randomly among different values in sending out each pulses. Equivalently, we can regard pulses of different intensities as pulses from different sources. For example, in a 3-intensity protocol[12], Alice has three sources, source Y_0 (vacuum source) which is supposed to produce vacuum only, source Y (decoy source) which is supposed to only produce state

$$\rho = \sum_{k=0}^{J} a_k |k\rangle\langle k| \tag{1}$$

only, and source Y' (signal source) which is supposed to only produce state

$$\rho' = \sum_{k=0}^{J} a'_k |k\rangle\langle k|, \tag{2}$$

where $|k\rangle$ is the $k-$photon Fock state and $a_k \geq 0,\ a'_k \geq 0$ for all k, $\sum a_k = \sum a'_k = 1$. Here J can be either finite or infinite. Given a coherent-state source or a heralded single-photon source from the parametric down conversion, $J = \infty$.

The fundamental formula in the decoy-state method as first proposed by Hwang[11] is that the counting rates (yields) of pulses of the same photon-number states must be equal to each other even they are from different source, i.e.

$$s_k = s'_k \tag{3}$$

where s_k and s'_k are counting rate of $k-$photon pulses from the decoy source and counting rate of $k-$photon pulses from the signal source, respectively. This is because of the obvious

fact that those $k-$photon pulses from different sources are actually *randomly* mixed therefore they are *random samples* of each other, *if* sources Y_0, Y, Y' are perfectly stable, i.e., they always produce a state precisely as the assumed one. Given Eq.(3), one can list simultaneous equations[12] for s_k based Eqs.(1,2) and then find out the lower bound of s_1 (s_1') which indicates the lower bound of single photon counts of the decoy source and signal source.

Given this, one can calculate the final key rate of each source, by the well known result of ILM-GLLP[4, 5]. For example, the asymptotic final key rate for the signal source can be calculated by

$$R_s = \Delta_1'[1 - H(t_1)] - H(t) \tag{4}$$

where t_1, t are the QBER for single-photon counts of the signal source and the QBER for all counts of the signal pulses from the signal source. Δ_1' is the lower bound of the fraction of counts due to single photon pulses from the signal source. Moreover, the non-asymptotic unconditional secure key rate in a finite-size QKD is extensively studied recently, first in Ref.[4], and then further studied in [6, 7].

Recently, a number of QKD experiments using the decoy-state method have been done [21, 22, 23, 24, 25]. However, the story is not completed here because the existing decoy-state theory does not entirely cover the real experimental conditions in practice. No source in real-life can be perfectly stable. One important problem is the effect of source errors. Suppose in a protocol Alice sends out M pulses one by one. The actually produced state at any time i can differ from the assumed state that she *wants*. We call this discrepancy *source error*. Say, at any time i, Alice *wants* to prepare a state

$$\rho_i = \sum_{k=0}^{J} f_k |k\rangle\langle k| \tag{5}$$

for Bob, but the source actually prepares a slightly different state

$$\tilde{\rho}_i = \sum_{k=0}^{J} f_{ki} |k\rangle\langle k| \tag{6}$$

in the Fock space. We shall call such $f_{ki} - f_k$ source error, or state error, or parameter fluctuation. Most generally, the error, $f_{ki} - f_k$ is *not* random for different i. In practice, one of the major cause of the source error is the intensity fluctuation. Therefore we often use the term *intensity fluctuation* for the source errors. But our result here is not limited to the intensity fluctuation only. Here we consider a more general case that the parameters in

the state fluctuate. Therefore we shall still use the term *source error* in stead of intensity fluctuation.

If the source error is random, we can simply assume a perfectly stable source always emitting the averaged-state[14, 26] of all pulses from a certain source. As shown in Ref.[26], we have to take a feed-forward control to each individual pulses in order to guarantee the randomness of source errors. If we use coherent light only, and if we have a stable two-value attenuator, we can use the method in Ref.[27] to manage any intensity fluctuations.

If we don't assume any conditions above, the issue need to be studied more carefully. A very tricky point here is that the elementary assumption of Eq.(3) for the decoy-state method with stable sources is in general incorrect, if the state errors are *not* random. As we have shown explicitly[10, 28], there are cases that Eve. may know the source errors and she can violate Eq.(3) by producing an instantaneous transmittance channel dependent on the errors. Therefore, we must seek a solution to the new problem.

Very recently[28], a general asymptotic theory for decoy-state QKD with source errors is presented. By the method[28], we don't have to change anything in the existing set-up. The only thing we need is the bound values of a few parameters in the states from each source. However, that work has only presented the asymptotic result i.e., the effect of *classical statistical fluctuation* is not considered. Besides Ref.[28], the problem is also studied studied[29] asymptotically from another viewpoint for the Plug-and-Play protocol. There[29], Alice receives a pulse, attenuates it and sends it out for Bob. Eve controls both the incident pulse and the outcome pulse. Alice's transmittance γ in doing attenuation can be either γ^D or γ^S, depending on whether she wants to prepare a decoy pulse or a signal pulse. Similar to Ref.[27], Ref.[29] also assumes that Alice can do the two-value attenuation exactly. The fundamental formula assumed there [29]is

$$Y^D_{m,n} = Y^S_{m,n}$$

where $Y^D_{m,n}(Y^S_{m,n})$ is the counting rate of a decoy(signal) pulse which contains m photons when flying into Alice lab and contains n photons when flying away from Alice's lab, after Alice's attenuation. As was pointed out by the authors of Ref.[29], the effects of the internal fluctuation of Alice's lab was not considered there and also the validity of elementary equation $Y^D_{m,n} = Y^S_{m,n}$ is not studied[30]. Actually, as shown in the appendix of this work, the elementary equation does not always hold if there are fluctuations to Alice's attenuation.

Here in this paper, we study the effects of *both* source errors *and* classical statistical fluctuations. The existing works[28, 29] have not included the effect of statistical fluctuations in calculating the final key rate, though the effect can be included in principle. Our earlier work assumes zero error for vacuum source Y_0, here we shall assume errors in this source, besides errors in source Y and source Y'. Similar to the results in [28], the results presented here only need the bound values of a few parameters in the states of different sources. In particular, in deriving the fraction of single-photon counts we don't use any unproven assumption and we don't need worry about the internal fluctuation of any Alice's device, since our method *only needs the bound values of a few parameters in the source state*. We don't need to presume any specific distribution for our states. In our study in this work, classical statistical fluctuation is considered by estimating the observed values from the asymptotic values with a fixed standard deviation. We shall start with a protocol with one-way quantum communication only. But as we point out in the end of this paper, our method obviously also applies to a Plug-and-Play protocol.

This paper is arranged as the following. After the introduction above, we present our method with some important mathematical relations section II. We then present our main results in section III: the asymptotic and non-asymptotic formula for the fraction of single photon counts of the 3-intensity protocol with errors in states of all 3 sources. Some remarks on the source errors are addressed in section IV. The paper is ended with a concluding remark.

II. OUR METHOD

We assume that Alice sends M pulses to Bob one by one in the protocol. Each pulse sent out by Alice is randomly chosen from one of the 3 sources Y_0, Y, Y' with constant probability p_0, p, p', respectively. Each source has errors. Clearly, pM, $p'M$ and p_0M are just the number of the decoy pulses, the number of the signal pulses, and the number of pulses from the vacuum source, respectively. We assume we know the bounds of parameters in the states of each sources.

Our goal is to find out the lower bound of the fraction of counts caused by those single-photon pulses for both the signal source and the decoy source. The following quantities are directly observed in the protocol therefore we regard them as known parameters: N_d, the

number of counts caused by the decoy source, N_s, the number of counts caused by the signal source, and N_0, the number of counts caused by the vacuum source, Y_0. For our goal, we only need to formulate the number of counts caused by those single-photon pulses from each sources in terms of the known quantities N_0, N_d, N_s and p_0, p, p' and the bound values of those parameters of states in each sources.

A. Virtual protocol

For clarity, we first consider a virtual protocol;
Suppose Alice will send M pulses to Bob in the whole protocol. At any time i ($i \in [1, M]$), each source produces a pulse. The states of the pulses from sources Y_0, Y , Y' are

$$\rho_{0i} = \sum_{k=0}^{J} b_{ki} |k\rangle\langle k|, \tag{7}$$

$$\rho_i = \sum_{k=0}^{J} a_{ki} |k\rangle\langle k| \ ; \text{ and} \tag{8}$$

$$\rho'_i = \sum_{k=0}^{J} a'_{ki} |k\rangle\langle k|. \tag{9}$$

Here b_{0i} is a bit smaller than 1, and we assume b_0^L, lower bound of all b_{0i} is known in the protocol; ρ_i and ρ'_i are a bit different from ρ and ρ' of Eq.(1, 2), which are the assumed states in the perfect protocol where there is no source error. At any time i, only one pulse is selected and sent out for Bob. The probability of selecting the ith pulse source Y_0, Y or Y' is constantly p_0, p, and p' for any i. The un-selected two pulses at each time will be discarded. After Bob has completed all measurements to the incident pulses, Alice checks the record about which pulse is selected at each time, i.e., which time has used which source. Obviously, Alice can decide which source to be used at each time in the very beginning. This is just then the real protocol of the decoy-state method.

As shown below, based on this virtual protocol, we can formulate the number of counts from each source and therefore find the lower bound of the number of single-photon counts. The result also holds for the real protocol where Alice decides to use which sources at the ith time in the very beginning.

B. Some definitions

Definition 1. In the protocol, Alice sends Bob M pulses, one by one. In response to Alice, Bob observes his detector for M times. As Bob's ith observed result, Bob's detector can either click or not click. If the detector clicks in Bob's ith observation, then we say that "the ith pulse from Alice has caused a count". We disregard how the ith pulse may change after it is sent out. When we say that Alice's ith pulse has caused a count we only need Bob's detector clicks in Bob's ith observation.

Given the source state in Eqs.(8,9), any ith pulse sent out by Alice must be in a photon-number state. To anyone outside Alice's lab, it looks as if that Alice only sends a photon number state at each single-shot: sometimes it's vacuum, sometimes it's a single-photon pulse, sometimes it is a $k-$photon pulse, and so on. We shall make use of this fact that any individual pulse is in one Fock state.

Definition 2. Set C and c_k: Set C contains any pulse that has caused a count; set c_k contains any $k-$photon pulse that has caused a count. Mathematically speaking, the sufficient and necessary condition for $i \in C$ is that the ith pulse has caused a count. The sufficient and necessary condition for $i \in c_k$ is that the ith pulse contains k photons and it has caused a count. For instance, if the photon number states of the first 10 pulses from Alice are $|0\rangle,\ |0\rangle,\ |1\rangle,\ |2\rangle,\ |0\rangle,\ |1\rangle,\ |3\rangle,\ |2\rangle,\ |1\rangle,\ |0\rangle,$ and the pulses of $i = 2,\ 3,\ 5,\ 6,\ 9,\ 10$ each has caused a count at Bob's side, then we have

$$C = \{i|i = 2,\ 3,\ 5,\ 6,\ 9,\ 10, \cdots\};\ c_0 = \{i|i = 2, 5, 10, \cdots\};\ c_1 = \{i|i = 3, 6, 9, \cdots\}. \quad (10)$$

Clearly, $C = c_0 \cup c_1 \cup c_2 \cdots$, every pulse in set C has caused a count.

Definition 3. We use superscripts U, L for the upper bound and lower bound of a certain parameter. In particular, given any $k \geq 0$ in Eqs.(7,8, 9), we denote x_k^L, x_k^U for the minimum value and maximum value of $\{x_{ki}|\ i \in c_k\}$; and $x = b, a, a'$. We assume these bound values are known in the protocol.

C. Some important relations and facts

If the ith pulse is an element of c_k, the probability that it is from Y_0, Y or Y' is

$$\mathcal{P}_{vi|k} = \frac{p_0 b_{ki}}{p_0 b_{ki} + p a_{ki} + p' a'_{ki}},$$

$$\mathcal{P}_{di|k} = \frac{pa_{ki}}{p_0 b_{ki} + pa_{ki} + p'a'_{ki}},$$
$$\mathcal{P}_{si|k} = \frac{p'a'_{ki}}{p_0 b_{ki} + pa_{ki} + p'a'_{ki}}. \tag{11}$$

We want to formulate the numbers of k-photon counts caused by each sources. Given the definition of the set c_k, this is equivalent to ask how many of pules in set c_k come from each sources. If the ith pulse contain k photons, it can come from any of the 3 sources, Y_0, Y or Y'. According to Eqs.(7, 8, 9), if the ith pulse contains k-photons, the probability that it comes from source Y_0 is

$$\mathcal{P}_{vi|k} = \frac{b_{ki} p_0}{p_0 b_{ki} + pa_{ki} + p'a'_{ki}}.$$

Or, equivalently,

$$n_{k0} = \sum_{i \in c_k} \mathcal{P}_{vi|k}.$$

Given a finite number of pulses and counts, this equation should be replaced by the expectation-value equation as

$$\langle N_0 \rangle = \sum_{k=0}^{J} \sum_{i \in c_k} \mathcal{P}_{vi|k} \tag{12}$$

This is the expected number of counts caused by source Y_0, since every pulse in $\{c_k\}$ has caused a count. Therefore we can formulate the expected value of the number of counts caused by source Y_0 by

$$\langle N_0 \rangle = \sum_{k=0}^{J} \sum_{i \in c_k} b_{ki} p_0 d_{ki} = \langle N_0^* \rangle + \sum_{k=1}^{J} \sum_{i \in c_k} b_{ki} p_0 d_{ki} \tag{13}$$

Here

$$d_{ki} = \frac{1}{p_0 b_{ki} + pa_{ki} + p'a'_{ki}}. \tag{14}$$

N_0 is the number of counts due to pulses from source Y_0, $N_0^* = p_0 \sum_{i \in c_0} b_{0i} d_{0i}$ is the number of counts due to those vacuum pulses from source Y_0. Similarly, if the ith pulse contains k photons, it has a probability $\mathcal{P}_{di|k} = \frac{pa_{ki}}{p_0 b_{ki} + pa_{ki} + p'a'_{ki}}$ to be from the decoy source, and a probability of $\mathcal{P}_{si|k} = \frac{p'a'_{ki}}{p_0 b_{ki} + pa_{ki} + p'a'_{ki}}$ to be from the signal source. Therefore we have

$$\langle n_{kd} \rangle = \sum_{i \in c_k} \mathcal{P}_{di|k} = \sum_{i \in c_k} pa_{ki} d_{ki}, \tag{15}$$

for the expected number of counts caused by those k-photon pulses from the decoy source, and

$$\langle n'_{ks} \rangle = \sum_{i \in c_k} \mathcal{P}_{si|k} = \sum_{i \in c_k} p'a'_{ki} d_{ki}, \tag{16}$$

for the expected number of counts caused by those k-photon pulses from the signal source. Therefore, besides Eq.(13) we also have the following 2 equations for $\langle N_d\rangle$ and $\langle N_s\rangle$ as the expected values of the number of counts due to the decoy pulses and signal pulses:

$$\langle N_d\rangle = \sum_{k=0}^{J}\sum_{i\in c_k}\mathcal{P}_{di|k} = p\sum_{k=0}^{J}\sum_{i\in c_k} a_{ki}d_{ki} \tag{17}$$

$$\langle N_s\rangle = \sum_{k=0}^{J}\sum_{i\in c_k}\mathcal{P}_{si|k} = \sum_{k=0}^{J}\sum_{i\in c_k} a'_{ki}d_{ki} \tag{18}$$

Here we have used Eqs.(15, 16).

For simplicity, we define

$$D_k = \sum_{i\in c_k} d_{ki} = \sum_{i\in c_k}\frac{1}{p_0 b_{ki} + p a_{ki} + p' a'_{ki}}. \tag{19}$$

Recall Eqs.(16,15), $\langle n'_{0s}\rangle$, $\langle n_{0d}\rangle$ are the expected number of pulses from the decoy source and signal source in set c_0.

Based on the formulas and definitions above, we find the following important facts:

Fact 1:

$$pa_0^U D_0 \geq \langle n_{0d}\rangle \geq pa_0^L D_0;\;\; p'a_0'^U D_0 \geq \langle n'_{0s}\rangle \geq p'a_0'^L D_0. \tag{20}$$

This is directly deduced from Eqs.(15,16).

Fact 2:

$$\frac{\langle N_0\rangle}{b_0^L p_0} \geq D_0 \geq \frac{a_1^L}{p_0\left[a_1^L - a_0^L(1-b_0^L)\right]}\left(\langle N_0\rangle - \frac{p_0(1-b_0^L)}{pa_1^L}\langle N_d\rangle\right). \tag{21}$$

Proof: Obviously,

$$D_0 \leq \frac{\langle N_0\rangle}{b_0^L p_0}. \tag{22}$$

On the other hand, since any $b_{0i}\leq 1$,

$$p_0 D_0 \geq \langle N_0\rangle - p_0\sum_{k=1}^{J}\sum_{i\in c_k} b_{ki}d_{ki} \geq \langle N_0\rangle - p_0\sum_{k=1}^{J} b_k^U D_k \tag{23}$$

To lower bound D_0, we only need upper bound $p_0\sum_{k=1}^{J} b_k^U D_k$. By Eq.(17) we know

$$p\sum_{k=1}^{J} a_k^L D_k \leq \langle N_d\rangle - \langle n_{0d}\rangle \tag{24}$$

which is equivalent to say

$$p_0\frac{b_1^U}{a_1^L}\sum_{k=1}^{J} a_k^L D_k \leq \frac{p_0 b_1^U}{pa_1^L}\left(\langle N_d\rangle - \langle n_{0d}\rangle\right) \tag{25}$$

We assume

$$\frac{a_k^L}{b_k^U} \geq \frac{a_1^L}{b_1^U}. \tag{26}$$

This condition can obviously hold if each pulses of source Y_0 is in an extremely weak coherent state. These conditions mean

$$p_0 \sum_{k=1}^{J} b_k^U D_k \leq \frac{p_0 b_1^U}{p a_1^L} \left(p \sum_{k=1}^{J} a_k^L D_k \right) \tag{27}$$

Therefore, based on Eq.(23,25) we have

$$p_0 D_0 \geq \langle N_0 \rangle - \frac{p_0 b_1^U}{p a_1^L} \left(\langle N_d \rangle - \langle n_{0d} \rangle \right) \geq \langle N_0 \rangle - \frac{p_0 (1 - b_0^L)}{p a_1^L} \left(\langle N_d \rangle - \langle n_{0d} \rangle \right) \tag{28}$$

Combining *fact 1* with Eq.(28), we obtain the following important formula

$$D_0 \geq \frac{a_1^L}{p_0 \left[a_1^L - a_0^L (1 - b_0^L) \right]} \left(\langle N_0 \rangle - \frac{p_0 (1 - b_0^L)}{p a_1^L} \langle N_d \rangle \right). \tag{29}$$

This completes the proof of fact 2.

Fact 3:

$$D_1 \geq \mathcal{D}_1^L = \frac{a_2'^L \langle N_d \rangle / p - a_2^U \langle N_s \rangle / p' - \left(a_2'^L a_0^U - a_2^U a_0'^L \right) D_0}{a_1^U a_2'^L - a_1'^L a_2^U}. \tag{30}$$

Proof: The startpoint of our proof is Eqs.(17, 18) which can be rewritten into

$$\langle N_d \rangle = \langle n_{0d} \rangle + p a_1^U D_1 + p\Lambda - \xi_1 \tag{31}$$

$$\langle N_s \rangle = \langle n'_{0s} \rangle + p' a_1'^L D_1 + p'\Lambda' + \xi_2 \tag{32}$$

where

$$\Lambda = \sum_{k=2}^{J} a_k^U \sum_{i \in c_k} d_{ki};\ \Lambda' = \sum_{k=2}^{J} a_k'^L \sum_{i \in c_k} d_{ki}, \tag{33}$$

and

$$\xi_1 = p \left[a_1^U D_1 + \Lambda - \left(\sum_{i \in c_1} a_{1i} d_{1i} + \sum_{k=2}^{J} \sum_{i \in c_k} a_{ki} d_{ki} \right) \right] \geq 0$$

$$\xi_2 = p' \left[\sum_{i \in c_1} a'_{1i} d_{1i} + \sum_{k=2}^{J} \sum_{i \in c_k} a'_{ki} d_{ki} - \left(a_1'^L D_1 + \Lambda' \right) \right] \geq 0$$

According to the definition of Λ and Λ', we also have

$$\Lambda' = \frac{a_2'^L}{a_2^U} \Lambda + \xi_3 \tag{34}$$

and

$$\xi_3 = \Lambda' - \frac{a_2'^L}{a_2^U}\Lambda \tag{35}$$

Further, we assume the important condition

$$\frac{a_k'^L}{a_k^U} \geq \frac{a_2'^L}{a_2^U} \geq \frac{a_1'^L}{a_1^U}, \text{ for all } k \geq 2. \tag{36}$$

The first inequality above leads to

$$\xi_3 \geq 0 \tag{37}$$

as one may easily prove. With Eq.(34), Eq.(32) is converted to

$$\langle N_s \rangle = \langle n'_{0s} \rangle + p' a_1'^L D_1 + p' \frac{a_2'^L}{a_2^U}\Lambda + \xi_2 + p'\xi_3 \tag{38}$$

Given the Eqs.(31, 38), we can formulate D_1:

$$D_1 = \frac{a_2'^L\langle N_d\rangle/p - a_2^U\langle N_s\rangle/p' - a_2'^L\langle n_{0d}\rangle/p + a_2^U\langle n'_{0s}\rangle/p' + a_2'^L\xi_1/p + a_2^U(\xi_2 + p'\xi_3)/p'}{a_1^U a_2'^L - a_1'^L a_2^U}. \tag{39}$$

Since ξ_1, ξ_2, and ξ_3 are all non-negative, and $a_1^U a_2'^L - a_1'^L a_2^U \geq 0$ by the second inequality of Eq.(36), we now have

$$\begin{aligned} D_1 = \sum_{i\in c_1} d_{1i} &\geq \frac{a_2'^L\langle N_d\rangle/p - a_2^U\langle N_s\rangle/p' - a_2'^L\langle n_{0d}\rangle/p + a_2^U\langle n'_{0s}\rangle/p'}{a_1^U a_2'^L - a_1'^L a_2^U} \\ &\geq \frac{a_2'^L\langle N_d\rangle/p - a_2^U\langle N_s\rangle/p' - \left(a_2'^L a_0^U - a_2^U a_0'^L\right) D_0}{a_1^U a_2'^L - a_1'^L a_2^U} = \mathcal{D}_1^L. \end{aligned} \tag{40}$$

Here we have used *Fact 1* for the bound values of $\langle n_{0d}\rangle$, $\langle n'_{0s}\rangle$. To minimize D_1, we have replaced $\langle n_{0d}\rangle$ by its upper bound and $\langle n'_{0s}\rangle$ by its lower bound as given in *Fact 1*. This completes the proof of *fact 3*.

III. MAIN RESULTS

A. Asymptotic result

Given *Fact 3*, the minimum value of the number of counts caused by single-photon pulses from the signal-source (or the decoy-source) is simply

$$\langle n'_{1s}\rangle^L = p' a_1'^L D_1 \leq \langle n'_{1s}\rangle, \text{ (or } \langle n_{1d}\rangle^L = p a_1^L D_1 \leq \langle n_{1d}\rangle). \tag{41}$$

Therefore, we can now bound the fraction of single photon counts among all counts caused by the signal source

$$\Delta_1' \geq \frac{p' a_1'^L \mathcal{D}_1^L}{\langle N_s \rangle} = \frac{a_1'^L (a_2'^L \langle N_d \rangle p'/p - a_2^U \langle N_s \rangle - p' \left(a_2'^L a_0^U - a_2^U a_0'^L \right) D_0}{\langle N_s \rangle (a_1^U a_2'^L - a_1'^L a_2^U)}. \tag{42}$$

Here the range of D_0 is given by *fact 2* in the earlier subsection. We don't have to replace D_0 by its largest possible value to obtain the smallest possible Δ_1' at this moment. Instead, we shall do numerical calculation by Eq.(4) with all possible values of D_0 in the range given by *fact 2* and find the worst case result directly to the key rate. Define $S' = \frac{\langle N_s \rangle}{p'M}$ as the counting rate of the signal source, $S = \frac{\langle N_d \rangle}{pM}$ as the counting rate of the decoy source, $S_0 = \frac{\langle N_0 \rangle}{p_0 M}$ as the counting rate of source Y_0, and M is the total number of pulses as defined earlier, we can write the right-hand-side of the inequality in term of counting rates:

$$\Delta_1' \geq \frac{a_1'^L \left[a_2'^L S - a_2^U S' - (a_2'^L a_0^U - a_2^U a_0'^L) S_0 / b_0^L \right]}{S' (a_1^U a_2'^L - a_1'^L a_2^U)} \tag{43}$$

Similarly, we also have

$$\Delta_1 \geq \frac{a_1^L \left[a_2'^L S - a_2^U S' - (a_2'^L a_0^U - a_2^U a_0'^L) S_0 / b_0^L \right]}{S (a_1^U a_2'^L - a_1'^L a_2^U)} \tag{44}$$

for the minimum value of fraction of single-photon counts for the decoy source.

Eqs. (42, 43, 44) and conditions of Eq.(26,36) are the asymptotic results of this work.

B. Non-asymptotic results

Strictly speaking, Eqs.(41, 30) cannot be used in a real experiment where the number of pulses are always finite. Therefore, in any real experiment we have to consider the effect of statistical fluctuation besides the effect of source errors.

First, $\langle n_{1s}' \rangle^L = p' a_1'^L D_1 \geq p' a_1'^L \mathcal{D}_1^L$ in the formulas is the lower bound of the expected number of single photon counts of the signal source, but we actually need the lower bound of n_{1s}', the (deduced) observed value (i.e., the true value) of the number single photon counts of the signal source in a certain experiment. Of course, given the expectation value, $\langle n_{1s}' \rangle^L$, one can deduce the lower bound $n_{1s}'^L$ of the experimental value n_{1s}' by classical statistics:

$$n_{1s}' \geq n_{1s}'^L = \langle n_{1s}' \rangle - \delta_1. \tag{45}$$

To be sure that this bound is correct with a probability exponential close to 1, we need set δ_1 considerably large, e.g.,

$$\delta_1 = 10\sqrt{\langle n'_{1s}\rangle}. \tag{46}$$

Here 10 standard deviation is chosen simply for convenience rather than a exact cut off point. As shown in Ref.[12], the probability that the statistical fluctuation exceeds this range is exponentially close to 0.

Second, in the right hand side of Eq.(30), there are many parameters of expectation values such as $\langle N_d\rangle, \langle N_s\rangle, \langle n_{0d}\rangle, \langle n'_{0s}\rangle$, which are *not* observed values in one specific experiment. We need to replace these parameters by the experimentally observed quantities to make the formula useful. Again, this can be done by using classical statistics. This is to say, we need consider the largest possible difference between the expectation values and the observed values due to the statistic fluctuations.

For clarity, we shall use $\langle\zeta\rangle$ for the statistical expectation value of observable $\hat{\zeta}$, and ζ for the true value or the observed value in the experiment. For example, we shall use $\langle n_{1d}\rangle$ for the expectation value of the number of counts at Bob's side due to the single-photon pulses from the decoy source at Alice's side. We shall also use the superscript U or L to indicate the maximum value or minimum value of certain variable. With the following condition,

$$\mathcal{P}_{vi|k} + \mathcal{P}_{di|k} + \mathcal{P}_{si|k} = 1, \text{ if } i \in c_k \tag{47}$$

for any k, we can now start to derive our non-asymptotic result. By classical statistics we know that there exists a real number δ_d satisfying

$$N_d = \langle N_d\rangle + \delta_d \tag{48}$$

with a probability exponentially close to 1 if we set

$$|\delta_d| \leq \delta_d^U = 10\sqrt{\langle N_d\rangle} \approx 10\sqrt{N_d}. \tag{49}$$

This indicates that

$$\langle N_d\rangle = N_d - \delta_d \tag{50}$$

with a probability exponentially close to 1 that δ_d is in the range given by Eq.(49). Also, there exists a real number δ_0 satisfying

$$\langle N_0\rangle = N_0 - \delta_0 \tag{51}$$

and $|\delta_0| \leq 10\sqrt{N_0}$.

In our problem, due to the constraint given in Eq.(47), the fluctuations of each variables are not independent. This can help us not to overestimate the effects of the fluctuations too much. Eq.(47) immediately leads to the following identity:

$$\langle N_s \rangle + \langle N_d \rangle + \langle N_0 \rangle = N_s + N_d + N_0. \tag{52}$$

This is to say, the total population in set C is fixed, but there could be fluctuation in the population distribution over sources Y_0, Y, Y'. Eq.(52), together with Eq.(50) and Eq.(51) leads to

$$\langle N_s \rangle = N_s - \delta_d - \delta_0. \tag{53}$$

We use

$$n'_{1s} \geq \tilde{n}'_{1s} = \langle n'_{1s} \rangle^L - 10\sqrt{\langle n_{1s} \rangle^L}. \tag{54}$$

This is the inequality for the experimental lower bound of the number of single-photon counts from decoy pulses, where

$$\langle n'_{1s} \rangle^L = p' a_1'^L \mathcal{D}_1^L \geq \frac{p' a_1'^L \left[a_2'^L \langle N_d \rangle / p - a_2^U \langle N_s \rangle / p' - \left(a_2'^L a_0^U - a_2^U a_0'^L \right) \langle D_0 \rangle \right]}{a_1^U a_2'^L - a_1'^L a_2^U} \tag{55}$$

and $\langle N_d \rangle$, $\langle N_s \rangle$ are defined by Eqs.(50,53). The range of $\langle D_0 \rangle$ is given by *Fact 2* where the range of $\langle D_0 \rangle$ is given by Eq.(51). To have the lower bound value of n'_{1s} in Eq.(54) , we only need put the smallest value of $\langle N_d \rangle$ and largest possible values of $\langle N_s \rangle, \langle D_0 \rangle$ into Eq.(55). However, we don't have use the largest possible value of $\langle D_0 \rangle$, because we only need the worst-case result of the final key rate, rather than the worst-case result in each steps.

According to these we can lower bound the fraction of single-photon counts of the raw bits caused by signal pulses through equation:

$$\Delta'_1 \geq \frac{\tilde{n}'_{1s}}{N_s} \tag{56}$$

where $\tilde{n}'_{1s}$ is defined in Eq.(54) and the ranges of related variables in Eq.(54) can be calculated by Eq.(55,50,51,53) and *Fact 2*, if conditions of Eq.(26,36) hold.

For coherent states, if the intensity is bounded by $[\mu^L, \mu^U]$ for the decoy pulses and $[\mu'^L, \mu'^U]$ for the signal pulses then

$$a_k^X = (\mu^X)^k e^{-\mu^X}/k!, \; a_k'^X = (\mu'^X)^k e^{-\mu'^X}/k! \tag{57}$$

with $X = L,\ U$ and $k = 1, 2$ and

$$a_0^L = e^{-\mu^U},\ a_0^U = e^{-\mu^L}\ ; a_0'^L = e^{-\mu'^U},\ a_0'^U = e^{-\mu'^L} \tag{58}$$

Note that our result is not limited to a coherent state source. To calculate the unconditionally secure final key rate, one has to combine our result (eq.(56)) with the existing theory of finite-size QKD[4, 6, 7]. Here we make a loose treatment to show the effects of our Eq.(56) to the ket rate by adding statistical fluctuation to t and t_1 in Eq.(4). Detailed numerical results using the experimental data of QKD over 102.7 kilometers calculated by our formula is listed in table I. We treat the experimental data in the following way for key rate of the signal pulses by Eq.(4): (1)Δ_1' can be calculated by Eq.(56) as stated earlier. (2) Half of the experimental data of signal pulses should be discarded due to the measurement basis mismatch in the BB84 protocol. (3) Among the remaining half, a quarter of them are consumed for the bit-flip test and another quarter of them are consumed for the phase-flip test. (4) We use $t_0 = t_0(\mu') = 3.580\%$ as the observed value of both bit-flip rate and phase-flip rate. The final key is distilled from the remaining bits of signal pulses. The number of the remaining bits is not less than $\tilde{n}_{1s}'/4$. We use $t = t_0(\mu')$ for the bit-flip rate, and

$$t_1 = t_1' + 10\sqrt{4t_1'/\tilde{n}_{1s}'}. \tag{59}$$

and $\tilde{n}_{1s}'$ is given by Eq.(54), t_1' is

$$t_1' = \frac{t_0 - \frac{p' a_0'^L D_0}{2N_s'}}{\Delta_1'}. \tag{60}$$

We then put all possible values of D_0 into Eq.(4) according to *Fact 2* and Eq.(51) for the worst-case result of key rate over D_0.

The detailed experimental parameters can be founded in Ref.[22]. For completeness, we list the main parameters here in table II:

IV. SOME REMARKS ON THE SOURCE ERRORS

By the existing technology, one can indeed use whatever stabilizer to reduce the source errors considerably. Even with this fact, our theoretical results are still necessary: First, no technology can guarantee a perfectly stable source. It is also questionable whether any existing device has been proven to be able to reduce the source errors to a low level which

TABLE I: Secure key rate (final bits per pulse in the unit of 10^{-6}) vs intensity error upper bound using the experimental data in the case of 102.7 km [22]. The first row lists different values of upper bounds of intensity errors, δ_M, i.e., when we want an intensity x, we can actually create a pulse of any intensity in the range $[x(1-\delta_M),\ x(1+\delta_M)]$. Other rows list the final key rates, which are the numbers of final bits per signal pulse after error test, i.e., $\frac{n_f}{\tilde{N}_s}$ where $\tilde{N}_s$ is the number of raw bits of signal pulses after error test, n_f is the number of final bits distilled from these $\tilde{N}_s$ raw bits. R is the asymptotic key rate, R_1, R_2, R_3 are the non-asymptotic key rates with the intensity of each pulses in Y_0 being bounded by 0, 0.5%, 1%, respectively. The intensity fluctuations of any decoy-pulse and signal pulses are bounded by δ_M. In the table we have given the results of key rate while δ_M ranges from 0 to 3%.

δ_M	3%	2.5%	2%	1.5%	1%	0.5%	0
R (in 10^{-6})	11.03	12.09	13.15	14.19	15.23	16.26	17.28
R_1 (in 10^{-6})	1.536	2.567	3.591	4.607	5.616	6.618	7.614
R_2 (in 10^{-6})	1.506	2.537	3.561	4.577	5.587	6.589	7.585
R_3 (in 10^{-6})	1.475	2.507	3.531	4.548	5.557	6.560	7.556

TABLE II: Main parameters and observed results in the experiment of Ref[22]. M : total pulses sent out by Alice during the experimental time. $t_0(\mu)$, $t_0(\mu')$: quantum bit error rates (QBER) of decoy pulses and signal pulses. S', S, S_0: counting rates of the signal pulses, decoy pulses and Y_0 pulses.

From the results listed in table I, we find that the effects of source errors to the key rate is not significant (provided that the source error is not too large.) For example, in the asymptotic case (results in the first row), if the largest intensity fluctuation is controlled to be less than 0.5%, the key rate is decreased 17.28 Hz(the data in the last column of the first row) to 16.26 Hz only(the data in the second column from the right of the first row). However, the statistical fluctuation decrease the key rate significantly, given the existing experiment[22]. If we strictly considered the finite-size effect[4, 6, 7], the key rate would be further decreased. To reduce the effects, one can increase the number of pulses in the set-up.

M	$t_0(\mu')$	$t_0(\mu)$	S'	S	S_0	p'	p	p_0
5.222×10^9	3.580%	9.098%	1.262×10^{-4}	4.611×10^{-5}	6.711×10^{-6}	0.5	0.4	0.1

is exponentially close to 0. If *unconditional security* is our goal in practice, we must show *quantitatively* the effects of any polynomially imperfections. For example, even we can control the intensity fluctuation to be less than 0.5%, we had better still consider the effects of intensity fluctuation *quantitatively* rather than simply *trust* that the effects are negligible by *intuition*. Otherwise, one may ask why the cut off point is 0.5% rather than 0.0001% or 25% ? The security is then standardless. If we disregard the effect of source errors, possibly we shall encounter the following ridiculous story: Set-up A produces a key rate of 1k/s with source errors of less than 0.5%, set-up B produces a key rate of 20k/s with source errors of 25% over the same distance. Do we have to believe that set-up B is better ? With our theoretical results, such type of issue is immediately resolved because we can calculate the net final key rate after considering the effects of source errors. Second, with our theoretical results, we don't have to blindly take too much costs in improving the source quality. For example, with our results we now know with strict proof that source intensity fluctuation less than 0.0001% is not so necessary, since it only improves the key rate negligibly, if we can already control the errors less than 0.5%. Finally, there are cases Eve. can indeed know the intensity errors[28]. As explicitly shown in[10, 28], in such cases Eve. can then violates Eqs.(3) through producing a time-dependent channel transmittance. The situation of the Plug-and-Play is even more serious: Eve. can actually *prepare* the error of each pulse then she can violate Eq.(3) for sure.

V. CONCLUDING REMARK AND DISCUSSIONS

In summary, we have shown how to calculate the lower bound of the fraction of single-photon counts in the decoy-state quantum key distribution with both source errors and statistical fluctuations. By our method, all imperfections have been taken into consideration in the largest possible errors of a few parameters of the source states in the photon number space. Therefore we only need to know the bound values of a few parameters of sources instead of assuming exact values of any physical quantity. For example, we don't have to assume zero internal fluctuation of of Alice's attenuation as assumed by earlier works[27, 29].

Obviously, our result here directly applies to the so called Plug-and-Play protocol first proposed by Gisin *et al.*. As pointed out in Ref[31, 32], the so called Plug-and-Play protocol can be made secure if the attenuation factors can be accurately set[29, 33]. However, in

the Plug-and-Play protocol, Eve. actually knows the error of each individual pulse hence both the error-free decoy-state theory based on Eq.(3) fails. Also, as shown in the appendix, if the attenuation factors cannot be set accurately, the result of Ref.[29] also fails but our theory here works.

Also, in a Plug-and-Play protocol, Alice receives strong pulses from Bob and she needs to guarantee the exact intensity of the pulse sending to Bob. It is not difficult to check the intensity, but difficult to *precisely correct* the intensity of each individual pulses. Our theory here can help to make it easier[28]: Alice monitors each pulses. She may either choose to do crude corrections to the pulses or not do any corrections: She simply discards those pulses whose intensity errors are too large (e.g., beyond 2%), and then use our theory to distill the final key.

It should be interesting to combine our result with the existing theories on final key distillation in a finite size QKD[4, 6, 7] for the unconditional final key rate in the finite-size decoy state QKD with an unstable source.

Acknowledgement: This work was supported in part by the National Basic Research Program of China grant No. 2007CB907900 and 2007CB807901, NSFC grant No. 60725416, 60525201 and 60708023, and China Hi-Tech program grant No. 2006AA01Z420.

VI. APPENDIX

Here we show that the elementary assumption $Y^D_{m,n} = Y^S_{m,n}$ used in Ref.[29]is *incorrect* if the actively controlled attenuation factor is not stable. (Ref.[29] assumes a stable attenuation controlled actively.) For simplicity, we consider those pulses containing 10 photons when flying into Alice's lab and after Alice's attenuation, containing 1 photon when flying away from Alice's lab to Bob. Alice decides to randomly use her transmittance $\lambda = \lambda^D = 0.01$ to produce a decoy pulse and $\lambda = \lambda^S = 0.05$ to produce a signal pulse. However, due to whatever un-controlled cause, there are internal fluctuations of λ value at different times. Consider the following specific case: to some blocks of pulses (we call these blocks *strong blocks*), to all decoy pulses and signal pulses, the real transmittance is a bit larger than λ, the value that Alice *wants*, while in some other blocks (we call *weak blocks*) the real transmittance is a bit smaller than λ. Suppose the number of pulses in the strong blocks and that in the weak blocks are equal. In the strong blocks, Alice's real transmittance

for a decoy pulse or a signal pulse is $\lambda^{D+} = 1.01\lambda^D$ or $\lambda^{S+} = 1.01\lambda^D$ while in the weak blocks, Alice's real transmittance for a decoy pulse or a signal pulse is $\lambda^{D-} = 0.99\lambda^D$ or $\lambda^{S-} = 0.99\lambda^S$. Suppose every block contains millions of pulses therefore Eve can know whether a block is a strong block or a weak block by observe the averaged intensity of pulses in the block. This is to say, Eve can treat different blocks *differently*. Eve produces a channel transmittance of η^+ to each pulses in the strong blocks and another transmittance η^- to each pulses in weak pulses. Note that here Eve does not know which pulses are decoy pulses and which pulses are signal pulses. She treats *all* pulses in one block fixed way. Now we can directly calculate $Y^D_{10,1}$ and $Y^S_{10,1}$:

$$Y^D_{10,1} = \frac{\lambda^{D+}(1-\lambda^{D+})^9\eta^+ + \lambda^{D-}(1-\lambda^{D-})^9\eta^-}{\lambda^{D+}(1-\lambda^{D+})^9 + \lambda^{D-}(1-\lambda^{D-})^9} = \frac{1.01(1-1.01\lambda^D)^9\eta^+ + 0.99(1-0.99\lambda^D)^9\eta^-}{1.01(1-1.01\lambda^D)^9 + 0.99(1-0.99\lambda^D)^9} \tag{61}$$

$$Y^S_{10,1} = \frac{\lambda^{S+}(1-\lambda^{S+})^9\eta^+ + \lambda^{S-}(1-\lambda^{S-})^9\eta^-}{\lambda^{S+}(1-\lambda^{S+})^9 + \lambda^{S-}(1-\lambda^{S-})^9} = \frac{1.01(1-1.01\lambda^S)^9\eta^+ + 0.99(1-0.99\lambda^S)^9\eta^-}{1.01(1-1.01\lambda^S)^9 + 0.99(1-0.99\lambda^S)^9} \tag{62}$$

It's easy to see that in general $Y^D_{10,1} \neq Y^S_{10,1}$ if $\eta^+ \neq \eta^-$. For example, given that $\eta^+ = 5\eta^-$, numerical calculation shows that

$$\frac{Y^D_{10,1}}{Y^S_{10,1}} > 1.0025 \tag{63}$$

This counter example shows that in general the assumption $Y^D_{m,n} = Y^S_{m,n}$ is incorrect if Alice's transmittance is not exactly controlled. We have demonstrated this fact with a pulse containing 10 photons, one can also consider a pulse containing 10^7 photons and shall find very similar result: Eve. can make $Y^D_{10^7,1}$ significantly different from $Y^S_{10^7,1}$. This has clearly broken the elementary assumption used in [29]. Obviously, such a case is equivalent to say that the pulse intensity from Alice is inexact, this is just the case we have studied in [28]. As was clearly shown there and also in[10], Eve can produce different transmittance for the single-photon state from the decoy source and the signal source. If Alice can control the attenuation exactly, i.e., λ^D, λ^S, there exists more efficient way to manage the issue in the protocol of one-way quantum communication[27].

---

[1] C.H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing (IEEE, New York, 1984)*, pp. 175-179.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] M. Dusek, N. Lütkenhaus, M. Hendrych, in *Progress in Optics VVVX*, edited by E. Wolf (Elsevier, 2006).

[4] H. Inamori, N. Lütkenhaus, D. Mayers, European Physical Journal D, 41, 599 (2007), which appeared in the arXiv as quant-ph/0107017.

[5] D. Gottesman, H.K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[6] V. Scarani and R. Renner, Phys. Rev. Lett. 100, 302008 (2008) and also in 3rd Workshop on Theory of Quantum Computation, Communication, and Cryptography (TQC 2008), JAN 30-FEB 01, 2008 Univ Tokyo, Tokyo, JAPAN. See also in arXiv:0806.0120 .

[7] Raymond Y. Q. Cai and V. Scarani, New J. Phys., 11, 11, 045024 (2009), and also arXiv:0811.2628 .

[8] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H.P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).

[9] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).

[10] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Physics Reports **448**, 1 (2007)

[11] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[12] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).

[13] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A 72, 012326 (2005).

[14] J.W. Harrington *et al.*, quant-ph/0503002.

[15] W. Mauerer and C. Silberhorn, Phys. Rev. A **75** 050305 (2007); Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev.Lett. **99**, 180503 (2008).

[16] T. Hirikiri and T. Kobayashi, Phys. Rev. A (2006), 73, 032331; Q. Wang, X.-B. Wang, G.-C. Guo, Phys. Rev. A (2007), 75, 012312.

[17] M. Hayashi, New. J. Phys., **9** 284, 2007.

[18] R. Ursin *et al.*, quant-ph/0607182.

[19] V. Scarani, A. Acin, G. Ribordy, N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004); C. Branciard, N. Gisin, B. Kraus, V. Scarani, Phys. Rev. A **72**, 032301 (2005).

[20] M. Koashi, Phys. Rev. Lett., **93**, 120501(2004); K. Tamaki, N. Lükenhaus, M. Loashi, J. Batuwantudawe, quant-ph/0608082

[21] D. Rosenberg em et al., Phys. Rev. Lett. **98**, 010503 (2007).

[22] C.-Z. Peng *et al.* Phys. Rev. Lett. **98**, 010505 (2007).

[23] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).

[24] Z.-L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007); A.R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe, and A.J. Shields, Opt. Exp., 16, 18790 (2008).

[25] A. Tanaka *et al*, Opt. Exp., **16**, 11354 (2008).

[26] X.-B. Wang, Phys. Rev. A **75**, 012301(2007)

[27] X.-B. Wang, C.-Z. Peng and J.-W. Pan, Appl. Phys. Let. **90**, 031110(2007)

[28] X.-B. Wang, C.-Z. Peng, J. Zhang, L. Yang and J.-W. Pan, Phys. Rev. A, **77**, 042311 (2008).

[29] Y. Zhao *et al*, Phys. Rev. A **77**, 052327 (2008).

[30] As was discussed in the end of the conclusion section of Ref.[29]:" The security of practical QKD is a serious issue. It is very important to implement QKD system based on tested assumptions. There are still several crucial imperfections that are not analyzed in this paper. For example...How can we analyze the fluctuation of internal transmittance λ ? How can we test the key assumptions in our analysis, $Y^S_{m,n} = Y^D_{m.n}$?..."

[31] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320(2006).

[32] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. 96, 070502 (2006) ; Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, in Proceedings of IEEE International Symposium on Information Theory, Seattle, 2006, pp. 2094–2098 (IEEE, New York).

[33] X. Peng et al, Opt. Lett. 33, 2077 (2008).